JP7104976

Publication Title:

Pseudorandom number generator

Abstract:

A pseudorandom number generator which uses linear feedback shift registers and a nonlinear function circuit and can make the conditioned output distribution of generated pseudorandom numbers uniform even if the conditioned output distribution of the nonlinear function circuit has some deviation. The generator has a shift register to which the output of the nonlinear function circuit is inputted as a serial input, an initial value setting circuit for setting random initial values to the linear feedback shift registers and the shift registers, and an adder for adding predetermined bits of the parallel outputs of the register and outputting a pseudorandom number stream. The generator can be used to generate a cryptogram which cannot be deciphered by the correlation attack method.

---

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平7－104976

(43)公開日　平成７年(1995)４月21日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　7/58	A			
Ｇ０９Ｃ　1/00		9364－5L		
Ｈ０３Ｋ　3/84	A			

審査請求　有　請求項の数３　ＦＤ　（全　６　頁）

(21)出願番号　特願平5－274935

(22)出願日　平成５年(1993)10月６日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　島田　道雄
東京都港区芝５丁目７番１号　日本電気株式会社内

(74)代理人　弁理士　松浦　兼行

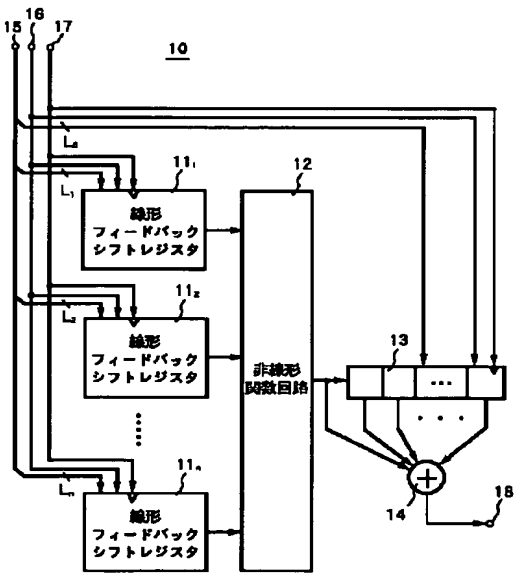
(54)【発明の名称】　擬似乱数発生装置

(57)【要約】

【目的】　本発明は暗号通信装置などで擬似乱数を発生するために用いられる擬似乱数発生装置に関し、コリレーションアタックによって初期状態を推定することが困難な擬似乱数発生装置を提供することを目的とする。

【構成】　複数の線形フィードバックシフトレジスタ１１$_1$～１１$_n$は互いに同一のクロックが入力されることにより同期して動作する。非線形関数回路１２は複数の線形フィードバックシフトレジスタ１１$_1$～１１$_n$の出力ビット列をそれぞれ非線形関数で結合する。シフトレジスタ１３は前記クロックの入力毎に記憶内容を１ビット右へシフトすると共に、非線形関数回路１２の出力１ビットを左端のビットに記憶する。加算器１４はシフトレジスタ１３の記憶ビットのうち予め定められた一部又は全部の記憶ビットと非線形関数回路１２の出力ビット列とを加算して擬似乱数を出力する。

本発明の一実施例の構成図



1

【特許請求の範囲】

【請求項1】　互いに同一のクロックが入力されることにより同期して動作する複数の線形フィードバックシフトレジスタと、

該複数の線形フィードバックシフトレジスタの出力ビット列をそれぞれ非線形関数で結合する非線形関数回路と、

前記クロックの入力毎に記憶内容を1ビット右へシフトすると共に、該非線形関数回路の出力1ビットを左端のビットに記憶するシフトレジスタと、

該複数の線形フィードバックシフトレジスタと該シフトレジスタにそれぞれ初期値を設定する設定手段と、

該シフトレジスタの記憶ビットのうち予め定められた一部又は全部の記憶ビットと該非線形関数回路の出力ビット列とを加算する加算器とを有し、前記クロックに同期して前記加算器より擬似乱数を出力することを特徴とする擬似乱数発生装置。

【請求項2】　前記複数の線形フィードバックシフトレジスタは、互いに全部又は一部が異なる長さのシフトレジスタをそれぞれ有することを特徴とする請求項1記載の擬似乱数発生装置。

【請求項3】　前記シフトレジスタは計算機による試行錯誤で初期値が判別できない長さであり、前記加算器は排他的論理和回路又は排他的否定論理和回路で構成されていることを特徴とする請求項1記載の擬似乱数発生装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は擬似乱数発生装置に係り、特に暗号通信装置などで擬似乱数を発生するために用いられる擬似乱数発生装置に関する。

【0002】

【従来の技術】従来より、電話、モデムあるいはテレビジョン放送などの通信システムにおける伝送情報が第三者によって盗聴されないようにするため、送信情報に擬似乱数を排他的論理和加算することにより送信情報を暗号化する暗号通信装置では、擬似乱数発生装置を用いる。この擬似乱数発生装置としては、従来より線形フィードバックシフトレジスタを用いたものなどが知られている（特開平2－90320号公報など）。

【0003】図2は従来の擬似乱数発生装置の一例の構成図を示す。この従来の擬似乱数発生装置は線形フィードバックシフトレジスタで、1982年にエージアン・パーク・プレスから発刊されたゴロム他著「シフトレジスタ・シーケンシーズ」（Solomon W. Golomb, Lloyd R. Weich, Richard M. Goldstein, and Alfred W. Hales, "Shift Register Sequences (Revised Edition)", Aegean Park Press, 1982）や、1993年に共立出版株式会社より発刊された岡本栄司著「暗号理論入門」などの文献に記載されている。

2

【0004】図2において、擬似乱数発生装置20はLビットのシフトレジスタ21と、排他的論理和回路22とよりなる。シフトレジスタ21は乱数入力端子23、モード制御信号入力端子24及びクロック入力端子25に接続され、また排他的論理和回路22の出力端子26に接続されており、入力端子24より入力されるモード制御信号が「1」のときに入力端子25よりクロックが1個入力されると、入力端子23より供給されるLビットの乱数を記憶する。

【0005】この擬似乱数発生装置（線形フィードバックシフトレジスタ）20を使用する前は上記のようにして、まず入力端子23よりのLビットの乱数を初期値としてシフトレジスタ21に記憶させておく。このシフトレジスタ21のLビットの出力のうち一又は二以上の予め定められた出力が排他的論理和回路22に供給される。排他的論理和回路22の出力信号はシフトレジスタ21のシリアル入力端子に入力される。

【0006】次に、擬似乱数を発生する時には、入力端子24より入力されるモード制御信号を「0」にし、入力端子25にクロックを供給する。シフトレジスタ21は入力端子24より入力されるモード制御信号が「0」のときに、入力端子25よりクロックが1個供給されると、記憶しているビット系列を右に1ビットシフトする。これにより、シフトレジスタ21に記憶されているLビットの情報のうち右端の1ビットが捨てられ、かつ、排他的論理和回路22の1ビットの出力信号がシフトレジスタの左端の1ビットに格納される。

【0007】以下、上記と同様にしてモード制御信号が「0」の状態のままクロックが入力される毎に、シフトレジスタ21の記憶ビット系列が1ビットずつ右へシフトされ、かつ、排他的論理和回路22の出力信号がシフトレジスタ21の左端のビットにその都度格納されていく。排他的論理和回路22の出力ビット系列はまた、出力端子26へ擬似乱数としてシリアルに出力される。

【0008】図3は従来の擬似乱数発生装置の他の例の構成図を示す。この従来の擬似乱数発生装置30は、1973年にエレクトロニクス誌1月号に掲載されたゲッフェの論文「ハウツー・プロテクト・データ・ウィズ・サイファーズ・ザット・アー・リアリィ・ハード・ツー・ブレイク」（Philip R. Geffe, "How to protect data with ciphers thatare really hard to break", Electronics, January 4, 1973, pp. 99－101）や、1993年に共立出版株式会社から発行された前記「暗号理論入門」などの文献に記載されている擬似乱数発生装置で、複数の線形フィードバックシフトレジスタ31

$_1$ ～３１$_n$の出力信号を非線形関数回路３２により結合して擬似乱数を発生して出力端子３６へ出力する構成である。

【０００９】複数の線形フィードバックシフトレジスタ３１$_1$ ～３１$_n$はシフトレジスタの長さは必ずしも等しくはないが、それぞれは図２と同様の構成であり、また、入力端子３３から初期値となるL$_1$ ビット、L$_2$ ビット、・・・、L$_n$ ビットの乱数がそれぞれ入力され、また入力端子３４からモード制御信号が共通に入力されると共に入力端子３５からクロックが共通に入力される構成とされている。

【００１０】非線形関数回路３２は入力と出力の関係が排他的論理和だけで表現できないような回路であり、論理回路で構成されることもあるし、リード・オンリ・メモリ（ROM）で構成されることもある。３入力（n＝３）の場合の非線形関数回路３２は例えば図４に示す如き回路構成とされる。同図において、非線形関数回路３２は２入力AND回路３２１及び３２３、インバータ３２２及び2入力OR回路３２４よりなる。

【００１１】AND回路３２１は入力端子３２５及び３２６を介して入力される１番目と２番目の２つの線形フィードバックシフトレジスタの出力ビット系列が入力されてそれらの論理積をとる。AND回路３２３は入力端子３２７を介して入力される３番目の線形フィードバックシフトレジスタの出力ビット系列と、入力端子３２６を介して入力される２番目の線形フィードバックシフトレジスタの出力ビット系列をインバータ３２２で極性反転したビット系列とが入力されてそれらの論理積をとる。OR回路３２４はAND回路３２１及び３２３の出力ビット系列の論理和をとり、その論理和信号を出力端子３２８（図３の３６）へ出力する。

【００１２】図３に示す従来の擬似乱数発生装置では、まず入力端子３４より線形フィードバックシフトレジスタ３１$_1$ ～３１$_n$へ「1」のモード制御信号を入力すると共に入力端子３５より１個のクロックを入力して、それぞれに入力端子３３よりの初期値となるL$_1$ ビット、L$_2$ ビット、・・・、L$_n$ ビットの乱数を格納する。次に、モード制御信号を「0」とし、入力端子３５を介してクロックを順次入力する。これにより図２と同様にして線形フィードバックシフトレジスタ３１$_1$ ～３１$_n$より乱数がシリアルに出力される。

【００１３】非線形関数回路３２はこれらの線形フィードバックシフトレジスタ３１$_1$ ～３１$_n$よりの各出力を非線形関数で結合して擬似乱数を生成し、その擬似乱数を出力端子３６へ出力する。

【００１４】

【発明が解決しようとする課題】しかるに、図２に示した従来の擬似乱数発生装置２０は擬似乱数系列の一部分がわかると、線形方程式をたてることで線形フィードバックシフトレジスタの初期状態が簡単に推定することができるという問題がある。

【００１５】これに対し、図３に示した従来の擬似乱数発生装置３０は非線形関数で結合した擬似乱数を出力するようにしているから、図２の従来装置２０に比し初期状態を推定することは困難であるが、これを送信データに擬似乱数を加算して暗号化する暗号通信装置に適用した場合は、もし非線形関数回路３２の入力の一部分を条件付けたときの出力分布に偏りがあると、コリレーションアタックあるいは系列相関と呼ばれる解読方法で解読できることが知られている（例えば、米国の電気電子技術者協会の１９８４年発刊の会誌に掲載されたシーゲンザラーの論文「コリレーション・イミュニティー・オブ・ノンリニアー・コンバイニング・ファンクションズ・フォア・クリプトグラフィック・アプリケーションズ」（T. Siegenthaler, "Correlation－Immunity ofNonlinear Combining Functions for Cryptographic Applications", IEEE Transactions on Information Theory, vol. IT－30, No. 5, pp. 776－780, September 1984）や、前記共立出版株式会社の１９９３年発刊の「暗号理論入門」参照）。

【００１６】コリレーションアタックで解読されないようにするには、非線形関数回路３２の条件付き出力分布を一様になるように設計すればよいのだが、非線形関数回路３２の入力が３ビットのようにビット数が少ない場合は、出力分布を一様にすることができない。従って、従来の擬似乱数発生装置３０では、安全で装置規模の小さな暗号通信装置が実現できないという問題がある。

【００１７】本発明は以上の点に鑑みなされたもので、コリレーションアタックによって初期状態を推定することが困難な擬似乱数発生装置を提供することを目的とする。

【００１８】

【課題を解決するための手段】本発明は上記の目的を達成するため、互いに同一のクロックが入力されることにより同期して動作する複数の線形フィードバックシフトレジスタと、複数の線形フィードバックシフトレジスタの出力ビット列をそれぞれ非線形関数で結合する非線形関数回路と、前記クロックの入力毎に記憶内容を１ビット右へシフトすると共に、非線形関数回路の出力１ビットを左端のビットに記憶するシフトレジスタと、複数の線形フィードバックシフトレジスタとシフトレジスタにそれぞれ初期値を設定する設定手段と、シフトレジスタの記憶ビットのうち予め定められた一部又は全部の記憶ビットと非線形関数回路の出力ビット列とを加算する加算器とを有する構成としたものである。

【００１９】

【作用】長さLビットの乱数に存在する「1」の数が奇

数個である確率は、「1」の発生確率が0でない限り、Lが大きくなるにつれて1／2に漸近する。従って、「0」、「1」の発生確率に偏りのある乱数をシフトレジスタに入力して記憶した後、そのシフトレジスタからの乱数を加算することにより、「0」、「1」の発生確率に偏りのない乱数を得ることができる。この方法は物理的な手段によって発生された乱数の出力分布を一様にするために使われる方法で、公知である（例えば、前記「暗号理論入門」参照）。

【0020】本発明はこの方法を利用するもので、非線形関数回路の出力ビット系列をシフトレジスタに入力し、非線形関数回路の出力ビット系列とシフトレジスタの全部又は一部のビット出力とを前記加算器により加算することにより、非線形関数回路の条件付き出力分布を一様にする。ただし、ある時刻におけるシフトレジスタの記憶状態がわかっていると、加算器の出力から非線形関数回路からシフトレジスタに新しく入力されるビットの値がわかる場合がある。従って、このような方法で非線形関数回路の条件付き出力分布を一様にして、上記の加算器の出力乱数を送信情報に加算して暗号化しても、シフトレジスタの初期状態（初期値）さえわかれば、依然としてコリレーションアタックにより暗号が解読されてしまう。

【0021】そこで、本発明では擬似乱数を発生する前に、シフトレジスタに前記設定手段により乱数を初期値として設定する。これにより、第三者は非線形関数回路の出力がわからなくなる。ただし、シフトレジスタの長さが短いと、試行錯誤によってシフトレジスタの初期値を推定することは可能であるため、シフトレジスタの長さは、計算機でしらみつぶしの試行錯誤によって初期値が推定できない程度の長さに設定する必要がある。

【0022】このように、本発明では、非線形関数回路の出力ビット系列をシフトレジスタと加算器により畳み込むことにより、擬似乱数を加算器より出力するようにしているため、条件付き出力分布に偏りのある非線形関数回路を用いても、擬似乱数の条件付き出力分布を一様にすることができる。

【0023】

【実施例】次に本発明の実施例について説明する。図1は本発明の一実施例の構成図を示す。同図において、擬似乱数発生装置10は、n個（ただし、nは2以上の整数）の線形フィードバックシフトレジスタ11_1～11_nと、線形フィードバックシフトレジスタ11_1～11_nの各出力ビット列を予め定められた非線形関数で結合する非線形関数回路12と、非線形関数回路12の出力ビット列が入力されるシフトレジスタ13と、シフトレジスタ13の予め定められた一部又は全部のビット出力と非線形関数回路12の出力ビット列とがそれぞれ入力されてこれらを加算する加算器14とより構成されている。

【0024】入力端子15は初期値となる乱数をn個の線形フィードバックシフトレジスタ11_1～11_nとシフトレジスタ13とに入力する。入力端子16はモード制御信号入力端子、入力端子17はクロック入力端子で、それぞれ線形フィードバックシフトレジスタ11_1～11_nとシフトレジスタ13とに共通に入力される。n個の線形フィードバックシフトレジスタ11_1～11_nは、それぞれ図2に示した構成と同様に、シフトレジスタとその出力のうち予め定められたビット出力を排他的論理和演算してシフトレジスタに入力すると共に出力する加算器とよりなるが、そのシフトレジスタの長さはそれぞれL_1ビット、L_2ビット、．．．．、L_nビットである。ここで、上記のL_1～L_nは例えばn＝5の場合、16ビットから30ビットまでのどれかに設定され、通常は互いに異なるように設定されるが、一部は同一の長さのものがあってもよい。

【0025】シフトレジスタ13はその長さがL_0ビットで、計算機のしらみつぶしの試行錯誤によって初期値が推定できないように最低でも30～60ビットの長さに設定される。加算器14は非線形関数回路12の出力ビット列と、シフトレジスタ13のL_0ビット並列出力のうち予め定められた一部又は全部の出力とが入力されてモジュロ2の加算を行う回路で、排他的論理和回路あるいは排他的否定論理和回路により構成されている。

【0026】次に本実施例の動作について説明する。まず、線形フィードバックシフトレジスタ11_1～11_nとシフトレジスタ13にそれぞれ入力端子16より「1」の値のモード制御信号が入力されると共に、入力端子17よりクロックが1個入力される。これにより、入力端子15に入力される$L_0+L_1+L_2+．．．+L_n$ビットの乱数のうち、L_1ビット、L_2ビット、．．．．、L_nビットの乱数部分がそれぞれ線形フィードバックシフトレジスタ11_1、11_2、．．．．、11_n内のシフトレジスタに初期値として格納され、かつ、シフトレジスタ13にL_0ビットの乱数部分が初期値として格納される。

【0027】加算器14は非線形関数回路12の出力ビットと、シフトレジスタ13のL_0ビットの初期値のうち予め定められた出力ビットとが入力されてモジュロ2の加算を行い、得られた加算結果を出力端子18へ出力する。

【0028】次に、入力端子16より線形フィードバックシフトレジスタ11_1～11_nとシフトレジスタ13にそれぞれ入力されるモード制御信号が「0」に切り換えられる。この状態で、線形フィードバックシフトレジスタ11_1～11_nとシフトレジスタ13にそれぞれ入力端子17を介してクロックが1個入力されると、線形フィードバックシフトレジスタ11_1～11_n内のシフトレジスタに記憶されている各初期値が1ビット右へシフトされて右端の1ビットが捨てられ、かつ、線形フィ

ードバックシフトレジスタ11_1～11_n内のシフトレジスタの左端の1ビットに内部の加算器の出力1ビットが格納されるとともに、外部の非線形関数回路12へ出力される。

【0029】これにより、非線形関数回路12は線形フィードバックシフトレジスタ11_1～11_n内のシフトレジスタに初期値が記憶されているときに出力されている最初の線形フィードバックシフトレジスタ11_1～11_nの各出力を非線形関数で結合して得た最初の値に続いて、上記の1ビットシフトに基づく2番目の各出力を非線形関数で結合して得た2番目の値を出力する。

【0030】一方、シフトレジスタ13は上記の線形フィードバックシフトレジスタ11_1～11_n内のシフトレジスタの動作と同様に、入力端子17を介してクロックが1個入力されると、記憶しているL$_n$ビットの初期値を1ビット右へシフトして右端の1ビットを捨て、かつ、左端の1ビットに非線形関数回路12の出力1ビット（上記の1番目の値）を取り込む。

【0031】加算器14は非線形関数回路12から出力される上記2番目の値と、1ビット右へシフト動作した後のシフトレジスタ13のL$_n$ビット並列出力のうち予め定められた出力ビットとが入力されてモジュロ2の加算を行い、得られた加算結果を出力端子18へ出力する。

【0032】以下、上記と同様にして、モード制御信号の値を「0」に保持したままで、例えば20MHzのクロックが入力される毎に出力端子18に擬似乱数が1ビットずつ出力される。ここで、上記のクロックは入力端子17を介して線形フィードバックシフトレジスタ11_1～11_nとシフトレジスタ13にそれぞれ共通に入力されるため、線形フィードバックシフトレジスタ11_1～11_nとシフトレジスタ13は同期して動作する。

【0033】このようにして、本実施例によれば、非線形関数回路12の出力ビット系列をシフトレジスタ13と加算器14により畳み込むことにより、擬似乱数を加算器14より出力するようにしているため、条件付き出力分布に偏りのある非線形関数回路12を用いても、擬似乱数の条件付き出力分布を一様にすることができ、従ってコリレーションアタックを用いても解読することができない暗号用の擬似乱数を生成することができる。

【0034】

【発明の効果】以上説明したように、本発明によれば、条件付き出力分布に偏りのある非線形関数回路を用いても、擬似乱数の条件付き出力分布を一様にすることができるため、装置規模の小さな3入力の非線形関数回路を用いても、コリレーションアタックによって解読できない暗号通信装置を実現できる。

【図面の簡単な説明】

【図1】本発明の一実施例の構成図である。

【図2】従来の一例の構成図である。

【図3】従来の他の例の構成図である。

【図4】非線形関数回路の一例の回路図である。

【符号の説明】

10　擬似乱数発生装置

11_1～11_n　線形フィードバックシフトレジスタ

12　非線形関数回路

13　シフトレジスタ

14　加算器

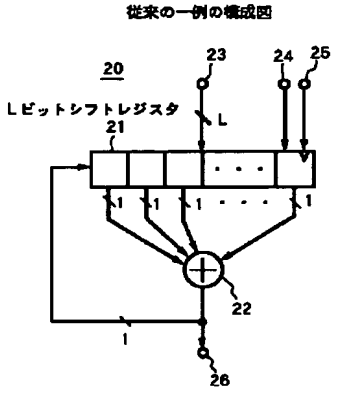
15　乱数入力端子

16　モード制御信号入力端子

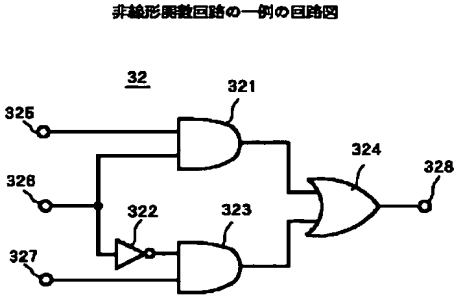
17　クロック入力端子

18　擬似乱数出力端子

【図2】

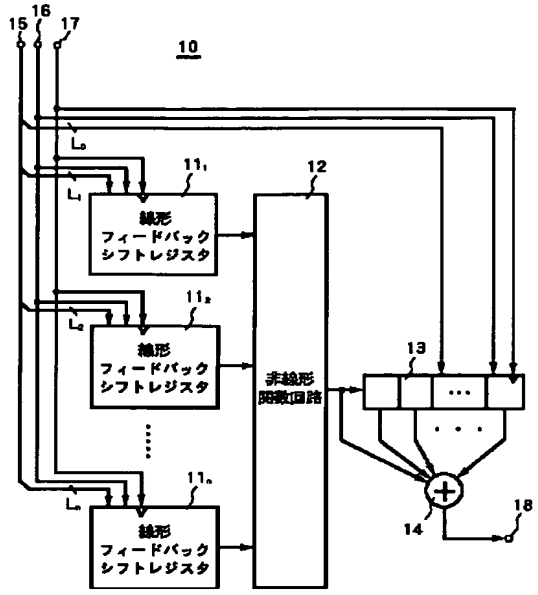


【図4】



【図1】

本発明の一実施例の構成図



【図3】

従来の他の例の構成図